Contents lists available at ScienceDirect

Technological Forecasting & Social Change

journal homepage: www.elsevier.com/locate/techfore

The effect of IT security issues on the implementation of industry 4.0 in SMEs: Barriers and challenges[1]

Marta F. Arroyabe[a], Carlos F.A. Arranz[b], Ignacio Fernandez de Arroyabe[c,d], Juan Carlos Fernandez de Arroyabe[a,*]

[a] Essex Business School, University of Essex, Elmer Approach, Southend-on-Sea, UK
[b] Greenwich Business School, University of Greenwich, Old Royal Naval College, Park Row, London, UK
[c] Computer Science, University of Loughborough, Loughborough, Leicestershire, UK
[d] Banking, Lloyds Banking Group, London, UK

ARTICLE INFO

Keywords:
Industry 4.0
Digitalisation
IT security issues
Barriers
Challenges
Industrial internet of things
ANN-MLP

ABSTRACT

Our paper explores how IT security issues affect the implementation of Industry 4.0 in small and medium-sized enterprises (SMEs) in the manufacturing sector. To develop this research question, we carry out an empirical study, with a survey of 3184 manufacturing SMEs, using the “Flash Eurobarometer No. 486” database from Eurostat (European Union). Using machine-learning methodology (ML), our contribution extends previous literature on the barriers to the digital transformation of SMEs, showing the role that IT security issues play in this process. Firstly, our findings indicate a positive association between IT security issues and the process of digitalisation within companies. These IT security challenges are perceived as catalysts for digital transformation, particularly in the context of SMEs. Secondly, our research reveals a significant degree of heterogeneity in the levels of digitalisation across companies. This spectrum ranges from firms at the forefront of digital technology integration, incorporating advanced elements like robotics, cloud computing, and smart devices, to another group of companies in the early stages of adopting Industry 4.0 technologies. Lastly, our study underscores the existence of a parallel relationship between IT security issues and the extent of digitalisation within SMEs. This connection highlights the intricate interplay between cybersecurity concerns and the level of digital maturity achieved by these businesses.

1. Introduction

Important initiatives can be found in the industrial sector, which seeks digital transformation, developing connectivity, intelligence and flexible automation, with the aim of improving the competitiveness of companies (Masood and Sonntag, 2020; Zhu et al., 2021; Uygun and Aydin, 2021). Thus, initiatives such as Industry 4.0 (I4.0), originating in Germany, Intelligent Manufacturing in the US, Made in China 2025, Future of Manufacturing in the UK and Smart Factory in South Korea (Liao et al., 2017; Frank et al., 2019; Horváth and Szabó, 2019; Galati and Bigliardi, 2019; Masood and Sonntag, 2020; Sanchez et al., 2020; Nounou et al., 2022) not only aim to improve the competitiveness of industries but also national economies. This digitalisation of industries is fundamentally based on industries assuming emerging technologies such as big data, cloud computing, artificial intelligence, and machine learning (AI/ML), robotics, data analytics and blockchain in an interconnected industrial environment through the Internet of Things (IoT) (Masood and Sonntag, 2020; Morkunas et al., 2019).

In this context, small and medium-sized enterprises (SMEs) are recognizing the impact of Industry 4.0, incorporating digital technologies in their processes, either to increase productivity (revenue or position in the market) or, encouraged by the supply chain, to meet the requirements of the development of Industry 4.0 (Müller et al., 2018; Horváth and Szabó, 2019; Masood and Sonntag, 2020; Uygun and Aydin, 2021; Singh et al., 2022). Moreover, despite the literature has investigated the digitalisation of SMEs, particularly addressing the

* Corresponding author.
E-mail addresses: mf17255@essex.ac.uk (M.F. Arroyabe), c.fernandezdearroyabearranz@greenwich.ac.uk (C.F.A. Arranz), I.Fernandez@lboro.ac.uk, ignacio.fernandez-de-arroyabe@lloydsbanking.com (I.F. Arroyabe), jcfern@essex.ac.uk (J.C.F. Arroyabe).

[1] This paper was supported by the UKRI Discribe Hub+, Digital Security by Design (DSbD) Programme, funded through the Economic and Social Research Council [ES/V003666/1].

https://doi.org/10.1016/j.techfore.2023.123051
Received 15 February 2023; Received in revised form 23 November 2023; Accepted 24 November 2023
Available online 2 December 2023

barriers, challenges, and benefits (Orzes et al., 2018; Stoldt et al., 2018; Masood and Sonntag, 2020), it is worth noting that research on I4.0 has predominantly centred around large corporations (Horváth and Szabó, 2019; Masood and Sonntag, 2020; Yu and Schweisfurth, 2020; Schönfuß et al., 2021). The most common barriers for SMEs to adopt digital technologies include limited financial resources and undefined economic benefits, cultural challenges that range from management lack of support to employee resistance, shortage of skilled employees and technical knowledge, weak IT infrastructure, technical hurdles like the absence of standards and uncertainty about system reliability, and legal concerns about data security (Orzes et al., 2018).

Additionally, recent studies have argued that the digitalisation of SMEs is not solely determined by internal factors but is also influenced by the ecosystems in which SMEs are embedded (Benitez et al., 2020; Kahle et al., 2020; Moeuf et al., 2018). For instance, these authors have highlighted that supply chains in the context of I4.0 become highly complex, involving numerous actors and interactions. Innovation ecosystems are collaborative networks within this context, providing SMEs with access to knowledge and skills and focusing on co-creating value within the supply chain (Benitez et al., 2020; Russell and Smorodinskaya, 2018). Therefore, a comprehensive research framework for investigating digitalisation must consider the ecosystem and interconnections of SMEs.

The implementation of I4.0 entails a high degree of interdependence and interconnectedness among firms. As highlighted by Benitez et al. (2020), I4.0 is built upon the connectivity provided by the Internet of Things (IoT) or Industrial Internet of Things (IIoT) and the utilization of various digital technologies such as cloud computing, big data, and artificial intelligence. These technologies facilitate the exchange of information among devices and equipment across firms (Lu, 2017). This heightened interconnectivity exposes firms to a greater risk of cybersecurity incidents. For instance, the adoption of digital technologies like big data involves the storage of vast amounts of information, making it a potential target for cyberattacks. Furthermore, the integration of industrial robots into the IIoT, the utilization of cloud computing, and the deployment of smart devices all present potential vulnerabilities susceptible to various forms of attacks. These attacks may include tampering attacks capable of distorting device addresses or denial-of-service (DoS) attacks that disrupt wireless connections (Clim, 2019; Humayun, 2021). In this evolving landscape, the significance of IT security issues has grown substantially within the digitalisation process (Fernandez de Arroyabe et al., 2023). This is especially crucial when considering the potential risks associated with the interconnection to IoT and the overall cybersecurity vulnerabilities faced by firms, as highlighted by Kotuszewski et al. (2021) and Clim (2019).

Our study explores the impact of IT security issues on the digitalisation of SMEs within the manufacturing sector. First, to address our research question, we conducted an empirical study encompassing 3184 SMEs in the manufacturing sector. We collected data through a survey utilizing the Flash Eurobarometer No. 486 database from Eurostat, which belongs to the European Union (EU). Second, in line with previous works (Clim, 2019; Mirtsch et al., 2020; Humayun, 2021), we assume that the digitalisation of companies implies a greater exposure to threats and potential IT security issues, as a consequence of the greater interconnection of these firms with the ecosystem. In this context, we must assume that although IT security issues have classically played a controversial role in SMEs since many SMEs do not consider themselves to be targets of IT security issues, the empirical evidence shows that they receive both automatic attacks, for the mere fact of being on the network or targeted attacks, for being part of a supply chain with large companies (Fernandez de Arroyabe and Fernandez de Arroyabe, 2021). Therefore, it is to be expected that SME manufacturing managers will be affected by IT security issues, either as a barrier that hinders the digital transformation or as a challenge that encourages this process, promoting the introduction of digital technologies, for example, the use of cloud computing or blockchain. Lastly, we assume the heterogeneity of digitalisation in SMEs. In the literature, it has been highlighted that the level of digitalisation varies depending on the SME, from cloud computing, for example, to high levels of complexity such as the use of collaborative robots (Masood and Sonntag, 2020). Therefore, it is to be expected that IT security incidents may have a differential effect on SME manufacturing, depending on the level of digitalisation.

2. Conceptual framework and literature review

2.1. I4.0 in SMEs: barriers and challenges

Industry 4.0 in companies involves the implementation of digital technologies to disruptively transform production systems, work organization and strategic decision-making (Díaz-Chao et al., 2021). In fact, digital technologies combined with production management systems are the key factors for digital transformation (Bai et al., 2021; Sanchez et al., 2020; de Sousa Jabbour et al., 2018), allowing an increase in efficiency and quality in manufacturing and supply chains by automating different aspects of production and manufacturing (Brenner and Hartl, 2021; Zhu et al., 2021). Moreover, digital transformation is often cited under the broad umbrella of Industry 4.0, as a consequence of the important implications it has for both business and society. Thus, Sanders et al. (2016, p. 816) define Industry 4.0 as "the fourth industrial revolution that applies the principles of cyber-physical systems, the Internet and future-oriented technologies and intelligent systems with improved human–machine interaction paradigms". Other authors emphasize the importance of interconnection in the digitalisation transformation. For example, Pan et al. (2015, p. 1537) point out that "Industry 4.0 represents the ability of industrial components to communicate with each other". Both interpretations emphasize the characteristics of communication and the interaction between humans and machines. In this paper, we follow the definition provided by Trappey et al. (2017), which conceptualizes I4.0 as a comprehensive framework that empowers manufacturing processes with elements of tactical intelligence. This empowerment is achieved through the incorporation of cutting-edge techniques and technologies such as the IoT, cloud computing, or big data, for example.

In this paper, to analyse the impact of IT security issues on the digitalisation of SMEs, we adopt the theoretical framework of innovation adoption theory (Rogers et al., 2014; Hameed et al., 2012; Van Oorschot et al., 2018; Blanchard et al., 2013; Damanpour and Schneider, 2006; Frambach and Schillewaert, 2002). Within this framework, the adoption of innovations within firms is perceived as a process characterized by inherent difficulties and barriers, which can originate from internal factors, such as financial constraints, knowledge gaps, or internal resistance, or they can be influenced by external factors, including uncertainty and a lack of regulatory frameworks. Hence, our research posits that the adoption of I4.0 by SMEs constitutes a process that is not immune to various barriers and challenges.

In reference to the obstacles encountered in the Industry 4.0 implementation process, we can find various groups of works in the literature. The first group of works points out that SMEs have greater limitations on financial resources and knowledge, which makes it difficult to tackle the digitalisation process (Brunswicker and Vanhaverbeke, 2015; Singh et al., 2022). Matt and Rauch (2013) point out that financial difficulties limit investments in manufacturing technologies. For their part, Türkeș et al. (2019) pointed out the lack of general knowledge about I4.0 is a key barrier for SMEs. Orzes et al. (2018) determined the barriers to digitalisation, identifying six main ones: economic and financial, cultural, competence and resources, legal, technical and the implementation process. Masood and Sonntag (2020) corroborate previous work, pointing out that limited financial resources, knowledge resources and technological awareness are the main barriers and challenges.

A second group of works highlighted the managerial and management barriers of SMEs in the digital transformation (Rauch et al., 2018; Moeuf et al., 2018; Da Silva et al., 2020). Goerzig and Bauernhansl

(2018) pointed out that SMEs often lack the skill set to plan and implement new technologies. In this same line, Moeuf et al. (2018), and Vrchota et al. (2019) point out a mismatch between the I4.0 theory and the specific requirements of SMEs, particularly in production, logistics and organization. Galati and Bigliardi (2019) identify that the digitalisation of SMEs must consider the flexibility of the productive system of SMEs, and the need to standardize processes. Thomas and Barton (2012) point out that company size is a critical factor in effective implementation, and this may cause hesitation to introduce advanced manufacturing technologies due to high risk. In this sense, we must highlight the work of Wang et al. (2016), which proposes a specific procedure to implement I4.0 within SMEs.

Third, recent research has incorporated supply chains as a pivotal factor in the digitalisation of companies. For instance, Benitez et al. (2020) and Kahle et al. (2020) have emphasized that supply chains in the context of I4.0 become highly complex, involving numerous actors and interactions. Benitez et al. (2020) point out that this complexity implies that the ecosystem created can be crucial, particularly for SMEs, where innovation ecosystems are collaborative networks focused on co-creating value. In this context, the literature has expanded its scope beyond investigating technology adopters in I4.0, i.e., the demand side, to also highlight the role of technology providers, including SMEs, in the context of I4.0 as adopters or providers (Benitez et al., 2020; Kahle et al., 2020). While the literature on technology adopters from the demand side has grown extensively, the role of SMEs as providers remains relatively limited (Benitez et al., 2020).

Lastly, a group of works highlights the role of cybersecurity in the digital transformation of firms (Clim, 2019; Humayun, 2021). In this sense, Clim (2019) points out that digital transformation in industries is facilitated by both information and digital technologies. In this context, industries are characterized both by automation and by the exchange of data throughout the value chain, constituting an interconnected system that facilitates the production of goods and services. In this context, the authors draw attention to the problem of interconnections, where the cybersecurity risks and vulnerabilities generated are an important problem for the companies. In fact, Humayun (2021) point out that IT security issues can be found, for example, in smart devices with wireline connections, or in each layer of IIoT architecture (the sensing layer, the network layer, the service/data layer and the application layer), where attacks such as DoS, wormhole attack or hijacking attack can affect communication and data. Moreover, Clim (2019) highlights that a source of vulnerabilities is those produced by open ports and preselected passwords, as well as faulty and inefficient mechanisms to receive automatic firmware updates.

2.2. IT security issues and SMEs

As we have pointed out, the objective of this research is to analyse how IT security issues affect the digitalisation of SME manufacturing. First, we have seen that the digital transformation of companies is carried out through the incorporation of digital technologies (big data, cloud computing, artificial intelligence and machine learning (AI/ML), smart devices, robotics, data analytics, and blockchain, among others), which implies the integration of intelligent machines, storage systems and smart production systems, through the use of wireless sensor networks, communication protocols, distributed control systems and cloud computing. All these systems are interconnected to the IoT or IIoT, facilitating the production of goods and services. Second, the interconnection of systems in the digitalisation transformation of SME manufacturing implies being exposed to cybersecurity risks, which involve a malicious act that can cause damage to the data stored in computer systems, or, in general, disrupt the operations of the companies (Ani et al., 2016; Babbar and Bhushan, 2020). That is, given the vulnerabilities of the systems and those generated by the interconnections, cybersecurity is expected to be a major challenge for the advancement of digital industrial transformation. In this context, digitalisation can be seen by companies as a barrier to their progress until achieving the implementation of I4.0. However, other companies may assume that this is a challenge, considering it so, which implies a greater implementation of digital technologies, to protect themselves. Therefore, we pose a first research question:

Research Question 1 (RQ1): How do the IT security issues affect the digital transformation (I4.0) of SME manufacturing?

We must take into account the heterogeneity among manufacturing SMEs, which can stem from various sources, including differences in company management, roles within the supply chain, and the resources and knowledge available to these SMEs (Masood and Sonntag, 2020). As a result, companies may exhibit varying levels of digitalisation. Within this context, it is reasonable to assume that different levels of digitalisation imply varying degrees of interconnection, potentially leading to differences in exposure to potential IT security issues. In this context, it is expected that the impact of IT security issues increases as digitalisation levels rise due to greater exposure.

However, this potentially increasing relationship may be disrupted by several factors affecting each level of digitalisation. For instance, some authors have highlighted that SMEs often start their digitalisation efforts in response to IT security issues (Mittal et al., 2018a, 2018b; Fernandez de Arroyabe and Fernandez de Arroyabe, 2021). Consequently, they may adopt secure storage alternatives like cloud computing to mitigate the risk of data breaches. The utilization of secure communication methods through high-speed infrastructure with encryption can also serve as a motivating factor for SMEs in their initial stages of digitalisation when incorporating digital technologies. On the other hand, as companies advance in their digitalisation journey, they tend to acquire competencies and implement organizational procedures aimed at mitigating vulnerabilities associated with cybersecurity incidents. Fernandez de Arroyabe et al. (2023) argue that digitalisation procedures and capabilities become integral components of cybersecurity systems. During these advanced stages of digitalisation, companies shift their focus from the potential IT security issues to the benefits associated with digitalisation. These benefits become a driving force in their digital transformation journey. For example, as highlighted by Masood and Sonntag (2020), SMEs with a high degree of digitalisation gain access to competitive advantages such as cost reduction and product quality improvement, among other benefits.

Therefore, given these different arguments, it becomes essential to analyse the relationship between IT security issues and the degree of digitalisation in SMEs, with an expectation of nuanced behaviour contingent on specific circumstances. In light of this, we introduce a second research question:

Research Question 2 (RQ2): How do IT security challenges influence the level of digitalisation (I4.0) in small and medium-sized enterprises (SMEs) within the manufacturing sector?

3. Methodology

3.1. Database

To empirically explore the research questions, we use the database from Eurostat, Flash Eurobarometer No. 486, which is conducted for the European Commission (Eurostat, 2022). This specific survey covers interesting topics, such as innovation, and digital technologies. The fieldwork was conducted between February and May 2020. Interviews were conducted by phone in their respective national languages.

As this study only focuses on manufacturing firms, we discarded all cases of companies that do not belong to the manufacturing sector. Therefore, the used sample is composed of 3180 SME firms from the manufacturing sector. The sample is dominated by SMEs. Two-fifths of the sample is composed of microenterprises with fewer than ten members of staff (41.7 %), and there are 821 firms with between ten and 49 employees and 747 firms with between 50 and 250 employees.

3.2. Measures

The first variable of our research model captures *digital technologies*. To do this, Flash Eurobarometer's questionnaire poses a multi-item question, using a relation of emerging technologies such as big data, cloud technology, artificial intelligence and machine learning (AI/ML), robotics, data analytics and blockchain (Morkunas et al., 2019; Harish et al., 2021). The question posed is: which of the following digital technologies has your enterprise adopted? The question contains these multi-item options: i) Artificial intelligence; ii) Cloud computing; iii) Robotics; iv) Smart devices; v) Big data analytics; vi) High-speed infrastructure; and vii) Blockchain.

The second variable is the *obstacles or barriers* that SMEs find in the digitalisation process. The questionnaire poses the following question: which of the following is a barrier to digitalisation in your enterprise? The typology of obstacles has been extracted from the literature on the digital transformation of SMEs, including financial obstacles, knowledge and IT security issues (Orzes et al., 2018; Stoldt et al., 2018; Masood and Sonntag, 2020). The question contains these items: i) A liable lack of financial resources; ii) A lack of skills, including managerial skills; iii) A lack of information technology infrastructure, such as a high-speed internet connection; iv) Regulatory obstacles; v) IT security issues; vi) Uncertainty about future digital standards; and vii) Internal resistance to change.

The third variable measures the intention for *planning and implementing* digital transformation in manufacturing SMEs. The next question, following the questionnaires is: which of the following options best describes your enterprise's approach to digital technologies? The question contains these multi-item options: i) Your enterprise does not need to adopt any digital technologies; ii) Your enterprise has adopted or is planning to adopt basic digital technologies such as email or a website, but not advanced digital technologies; iii) There is a need to introduce advanced digital technologies but your enterprise does not have the knowledge, skills or financing to adopt them; iv) There is a need to introduce advanced digital technologies and your enterprise is currently considering which of them to adopt; and v) There is a need to introduce advanced digital technologies and your enterprise has already started to adopt them.

3.3. Econometric methods

Regarding the first research question (RQ1), which aims to analyse the effect of IT security issues on the digital transformation of SME manufacturing, we will begin by examining this effect through regression analysis. Previous researchers have emphasized the predictive power and the understanding of relationships between variables using regression analysis, allowing us to quantify how changes in one variable are associated with changes in another. Regression analysis enables us to investigate the impact of obstacles and barriers on the digital transformation of SMEs by quantifying the variability of the dependent variable based on independent variables (see Tables 3 and 4).

As independent variables, we introduce the variable *obstacles*, while the dependent variables consist of one measuring the level of digitalisation (referred to as *digitalisation*) and the other indicating the intention for future digitalisation planning (referred to as *planning*). Following the methodology of Arranz et al. (2021), the *digitalisation* variable is constructed as a cumulative index of seven types of digital technologies (AI, cloud computing, robotics, smart devices, big data analytics, high-speed infrastructure, blockchain), which collectively measure the level of digitalisation among manufacturing SMEs. The econometric model used here is the ordinal logistics regression model (OLR), as the degree of digitalisation in SMEs is an ordinal variable, ranging from 0 to 7. Additionally, the *planning* variable is also ordinal, with a range from 1 to 5. Table 3 presents the results of the regression analysis.

Moreover, we will combine regression analysis with machine learning methods, more specifically artificial neural networks (ANN). That is, to the explanatory power of regression models in causal analyses, we want to add the exploratory power of ANN models, especially in the case of the existence of non-linear relationships between input variables and multiplicity of interactions (Alpaydin, 2021). Arranz et al. (2021) point out that ANN is a powerful tool when dealing with complex, high-dimensional data and tasks that involve pattern recognition and non-linear relationships. Their versatility and ability to handle diverse data types make them a valuable asset in many domains. Arranz et al. (2021) point out that the combination of both methods not only allows us to know which variables affect the dependent variable but also to know how they are influencing. Therefore, we have carried out this second analysis, to determine not only which obstacles have an impact, but also how the IT security variables impact concerning financial, knowledge and management obstacles. For this, we have used an artificial neural network (ANN), using a multilayer perceptron (MLP) (Fig. 1). Of all the ANN models, we have focused on MLP, because, in addition to allowing non-linear data relationships to be modelled, its universality and versatility have been demonstrated compared to other types of neural networks (Mohrotra, 1994), which means that, can learn and represent any mathematical function, which makes them suitable for a wide variety of modelling and prediction tasks, obtaining a high level of model robustness. The network architecture of an ANN-MLP has an input layer, hidden layers and an output layer.

Arranz et al. (2021) highlight that the combination of both methods not only enables to identification of which variables affect the dependent variable but also provides insights into how they exert their influence. To achieve this, we utilized an artificial neural network (ANN) with a multilayer perceptron (MLP) architecture (see Fig. 1). Among various ANN models, we specifically opted for MLP because of its capability to model non-linear data relationships. Its universality and versatility have been well-established compared to other types of neural networks (Mohrotra, 1994), implying that MLPs can learn and represent any mathematical function, interpreting them as suitable for a wide array of modelling and prediction tasks while maintaining a high level of model robustness. The network architecture of an ANN-MLP typically comprises an input layer, hidden layers, and an output layer.

To design the ANN-MLP architecture, we follow Wang (2007) and Arranz and Fernandez de Arroyabe (2010) (see Table 1). In the procedure of design of the ANN-MLP architecture, we can distinguish two key points: i) the choice of the number and size of the hidden layers, and ii) the choice of the learning algorithm. First, while the number of inputs and outputs of the proposed network is given by the number of available input and output variables, the number and size of hidden layers are determined by testing several combinations of the number of hidden layers and the number of neurons, using a *trial and error approach* (Ciurana et al., 2008; Mohrotra, 1997). That is, the selected architectures are tested with diverse activation functions, finding that the best

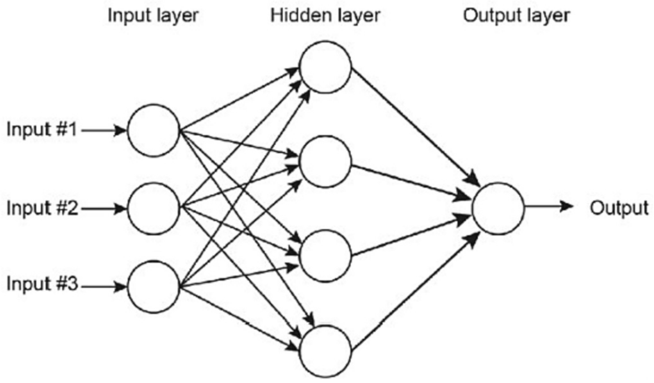


Fig. 1. ANN-MLP architecture.
Source: Arranz et al. (2021)

Table 1
Steps of the ANN procedure (Arranz et al., 2021).

1. Choice of the ANN typology

We choose the ANN architecture with Multilayer Perceptron (MLP).

2. ***Design of architecture of ANN-MLP***

- The network accuracy and efficiency are dependent on various parameters: hidden nodes, activation functions, training algorithm parameters and characteristics such as normalization and generalization.
- The number and size of hidden layers are determined by testing several combinations of the number of hidden layers and the number of neurons. The choice of an appropriate number of hidden neurons is extremely important; if few are used, few resources would be available to solve the adjustment problem and the use of too many neurons would increase the training time in addition to causing an overfit. Ciurana et al. (2008) and Mohrotra (1994) point out that for function approximation a two-layer neural network is usually sufficient to accurately model. Regarding the number of neurons in each hidden layer, Hegazy et al. (1994) proposed that the number of neurons should be 0.75 m or m, where m is the number of input neurons. Master (1993) established a rule that is based on the combination of input and output neurons. As a criterion, the number of units in the hidden layer should not exceed the number of input variables (Bishop, 1995). An extremely small number of units in the hidden layer compared to the number of input variables does not usually give a good result (Master, 1993; Bishop, 1995).
- The types of activation functions, typically, can be:
- For the hidden layer, we can use sigmoid logistic (values from 0 to 1) and a hyperbolic tangent (−1 to 1),
- For the output layer: softmax (identity) function.

3. The learning algorithm

Backpropagation. This learning algorithm determines the connection weights of each neuron, readjusting the weights and minimizing the error.

4. Learning stage

- To avoid problems of overfitting and consumption of processing time, we divided the sample randomly into three subsamples (*training, testing and holdout*).
- In the training stage, the weights and links between nodes are determined, to minimize the error. In the validation stage, the generalizability of the obtained architecture is checked. Lastly, the holdout data is used to validate the model.

4. Sensitive analysis

- A sensitive analysis is developed to quantify the influence of each input variable on the output variables.

architecture is one that minimizes the error. We have established the following models considering the input and output variables:

Model 1:

Digitalisation = f (lack of financial resources; lack of skills; lack of information technology infrastructure; regulatory obstacles; IT security issues; uncertainty about future digital standards; internal resistance).

Model 2:

Planning = f (lack of financial resources; lack of skills; lack of information technology infrastructure; regulatory obstacles; IT security issues; uncertainty about future digital standards; internal resistance).

The analytical equation of our simulation with ANN-MLP takes the following form for the case of the level of digitalisation:

$$Digitalization = h\left[\sum_{k=1}^{6}\alpha_k \bullet g\left(\sum_{j=1}^{6}\beta_{jk} \bullet X_j\right)\right]$$

with X_j being the input variable;

j the number of input variables;

$h(.)$ and $g(.)$ the hyperbolic tangent and softmax activation functions;

α_k and β_{jk} the input and hidden network weights, respectively;

k the number of hidden layers.

The results of both architectures for each model are shown in Table 2. Thus, for example, the architecture for the digitalisation level is 7–7-1, which means that there are 7, 7 and 1 neurons in the input, hidden and output layers, respectively. In the case of the hidden layer, the activation function used was the hyperbolic tangent and the softmax function was used for the output layer.

Table 2
ANN-MLP architecture for investment in cybersecurity analysis.

Output variable	ANN architecture	Activation functions	Error function
Digitalisation	7-7-1	• Hyperbolic tangent • Identity (Sofmax)	Cross-entropy
Planning	7-4-1	• Hyperbolic tangent • Identity (Sofmax)	Cross-entropy

Regarding the second research question (RQ2), IT security incidents have an effect depending on the level of digitalisation of SME manufacturing. For this, we analyse the existence of different behaviours/groups of companies depending on their digitalisation. We use the statistical model K-means cluster, which is widely used in data analysis and data mining due to its advantages and applications in a variety of contexts (Dudek, 2020; Mamat et al., 2018). Thus, K-means allows clustering of data into similar groups, which is useful when you have a large data set and want to discover underlying patterns or hidden structures in the data. In addition, K-Means is characterized by its versatility, since it can be applied to a wide variety of data types, such as numerical, categorical and mixed data, being very useful in many different applications. Finally, K-Means is computationally efficient and works well with large databases, its execution time being relatively fast, in relation to the amount of data and the number of clusters that must be found.

Using the K-mean cluster as a statistical model, we have proceeded in three stages. First, the K-mean input variables, we use the seven that measure the digital technologies adopted by SMEs. Second, we consider the analysis of K-mean, analysing the solutions from 2 clusters to 10 clusters. Solutions >10 clusters are hardly feasible considering that the input variables are two so the solution from 2 to 10 clusters includes all the possible combinations of the input variables. Third, we proceed to the choice of the most robust solution. For this, we use Silhouette analysis (Dudek, 2020; Mamat et al., 2018; Fraley and Raftery, 1998). This analysis allows us to determine the robustness of the cluster solution, the cohesion of each cluster and the separation of the groups. Silhouette index takes values in the interval [−1, 1], with values closer to 1 being the most robust solution. After proceeding to obtain the Silhouette index, the four clusters solution has a higher value (0.66). Furthermore, we performed a complementary analysis, using the Schwarz' Bayesian Criterion (Kass and Raftery, 1995; Fraley and Raftery, 1998), and the results confirm that the solution four clusters are the most robust in terms of cohesion and separation.

Once the manufacturing SMEs have been classified into various groups or clusters, we examine how each cluster affects the level of digitalisation, future digitalisation plans and IT security issues. For this, we use the ordinal logistic regression model as the econometric model. As dependent variables, we use the levels of *digitalisation*, *planning* and *IT security issues*. As independent variables, in both cases, we introduce the variable *cluster membership* as a categorical variable, each category being the groups and clusters. For the analysis of the results, the various regression coefficients must be interpreted as follows: the regression coefficient value 0 reflects the reference category ($cluster_i$), and the rest of the regression coefficients obtained correspond to the various categories ($cluster_j$) which reflect the probability of satisfaction level with respect to the first category. That is, H_0: ß ≤ 0 means there is a greater probability of satisfaction level of $cluster_i$ than $cluster_j$ in terms of digitalisation, and H_1: ß > 0 entails there is a greater probability of $cluster_j$ than $cluster_i$.

For the development of these research questions, we have utilized SPSS (Statistical Package for the Social Sciences), version 28. SPSS is a widely used software for statistical analysis and data analysis across various fields, including the performance of regression analysis and ANN.

4. Analysis and results

In our empirical analysis, we checked the robustness of the questionnaire and answers, testing the common method variance (CMV) and common method bias (CMB), following Podsakoff et al.'s method (2003). This analysis reveals six distinct latent constructs that account for 54.091 % of the variance. The first factor accounts for 18.118 % of the variance, which is below the recommended limit of 50 %. This result suggests CMV and CMB are not a concern in our results.

Regarding the first research question (RQ1), about the effect that IT security issues have on the digitalisation of companies, the results are shown in Table 3. Our results show that for the case of the cumulative index that measures the level of digitalisation, the IT security variable has a positive and significant coefficient (β = 0.522; $p < .001$), and in this same line, occurs for the planning of adoption of digital technologies (β = 0.315; p < .001), showing a positive effect. Table 4 presents the results for each of the seven digital technologies. While the regression coefficient for IT security issues is positive across all digital technologies, we observe variability in the impact of other obstacles depending on the technology. For example, in the case of artificial intelligence, the possession of IT infrastructure is an obstacle to digitalisation (β = −0.433; $p < .05$). In the context of cloud computing, obstacles such as internal resistance (β = 0.463; p < .001) and the presence of uncertainty (β = 0.309; $p < .01$), these are driving digitalisation. On the other hand, in the realm of robotics, both the need for financing (β = −0.299; p < .01) and internal resistance (β = −0.299; p < .01) act as impediments to technology adoption. Regarding the incorporation of smart devices, internal resistance (β = 0.365; p < .001) and the lack of IT infrastructure (β = 0.245; $p < .05$) promote adoption, while a lack of financing (β = −0.197; p < .001) serves as an obstacle. Organizational internal resistance proves to be a driver for big data adoption (β = 0.561; p < .001). In the case of high-speed infrastructure adoption, factors such as uncertainty (β = 0.221; p < .05) and internal resistance (β = 0.615; p < .001) act as motivators, while the absence of IT infrastructure (β = −0.620; p < .001) hinders adoption. Lastly, significant results for blockchain are found only in the case of IT security issues. Thus, while the diversity of obstacles varies in terms of their impact on digitalisation, it is evident that across all the models developed, IT security issues have a positive effect. In both tables, we have validated the robustness of the analysis, first, the significance of the model (p < .001); second, we have analysed both the autocorrelation (Durbin-Watson) and the existence of collinearity (VIF), and the results show acceptable values, confirming the robustness.

Table 3
Results of regression analysis (digitalisation and planning/obstacles).

	DIGITALISATION	PLANNING	VIF
FINANCE	−0.141*	−0.091	1.07
SKILLS	0.097	0.024	1.16
IT	0.024	0.140	1.08
REGULATORY	0.279**	0.049	1.14
IT SECURITY	0.522***	0.315***	1.23
UNCERTAINTY	0.240**	0.080	1.25
INTERNAL	0.605***	0.509***	1.14
−2 Log Likelihood	1684.30	1158.740	
Chi-Square	188.805	67.154	
Sig.	0.000	0.000	
Cox and Snell	0.058	0.027	
Nagelkerke	0.060	0.029	
McFadden	0.018	0.011	

* p < .05.
** p < .01.
*** $p < .001$.

In order to quantify the effect of IT security issues in relation to the rest of the obstacles, we have carried out modelling with ANN, establishing *obstacles* as input variables and *digitalisation* and *planning* as output variables. Focusing on the results of the simulation of the impact of IT security at the digitalisation level, Figs. 2 and 3 show the normalized importance of each input variable in the output variable.[2] We observe that IT security has the highest effect on the digitalisation level (IT security: 0.200; 100 % normalized value). Regarding the future adoption of new technologies (*planning*), we observe that the most important variables are financing (Finance: 0.289; 100 % normalized value), followed by IT security issues (IT security: 0.169; 58.5 % normalized value). Therefore, our results show the importance of IT security in the digitalisation of SMEs, with respect to the rest of the obstacles. We have tested the robustness of the analysis, and we can point out that the robustness of the simulation is high, considering the various tests performed. First, we tested the fitting of the ANN-MLP design, and it performed a level of fitting higher than 70 %. Second, we checked the predictability of our models, using the ROC curve, which is a figure of sensitivity versus specificity, showing the classification performance (Woods and Bowyer, 1997). That is, if the curve moves away from 45 degrees, the accuracy of the model is higher. In our case, the ROC curve shows that the chosen architecture can predict >60 % of the values of the output variable.

Regarding the second research question (RQ2), which investigates whether this effect varies depending on the level of digitalisation of SMEs, we conducted an exploratory analysis to categorize the different companies based on their degree of digitalisation. The results of the K-means clustering are displayed in Table 5, revealing that the most robust solution consists of four clusters, as determined by the Silhouette method. Furthermore, we conducted a robustness check of the analysis using ANOVA, which indicated a significant difference in the degree of digitalisation based on the cluster variable (Table 6).

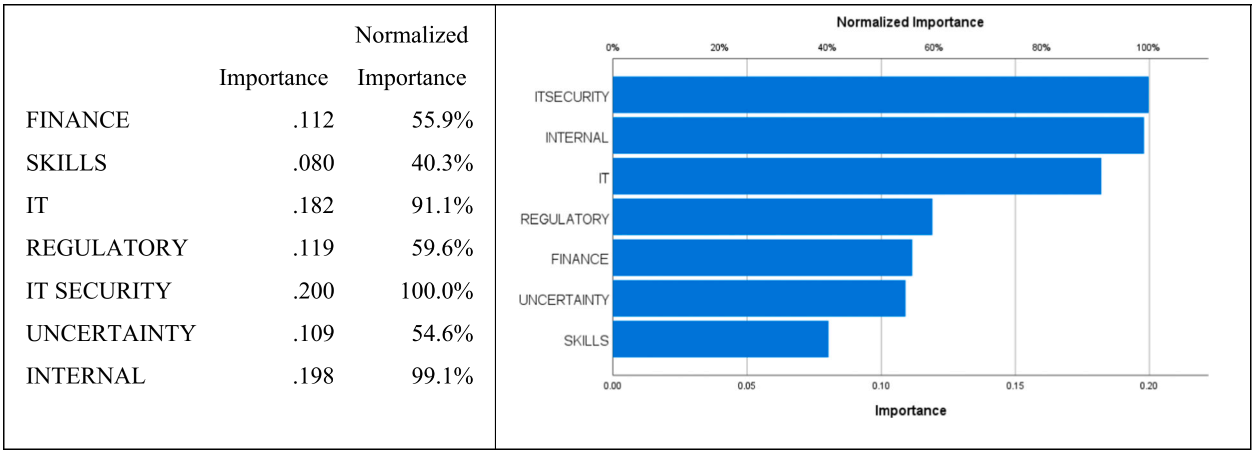
To characterize the four clusters based on the degree of digitalisation, Fig. 4 and Table 7 illustrate the differences among them, represented as the mean values of each digital technology within each cluster. For instance, there is perceptible variability in the adoption of digital technologies, with Cluster 4, consisting of 407 SMEs, exhibiting the highest degree of integration across all digital technologies, indicating a *high level of digitalisation*. Cluster 4 particularly stands out for its adoption of robotics (mean: 1), with all companies in this cluster having implemented robots. It is followed by smart devices (mean: 0.9287), cloud computing (mean: 0.7125), high-speed infrastructure (mean: 0.5872), big data (mean: 0.3833), and lastly, blockchain (mean: 0.0909). Cluster 1, comprising 675 SMEs, exhibits a lower degree of digitalisation compared to Cluster 4. However, all companies in Cluster 1 have implemented smart devices (mean: 1.000), and to a lesser extent, cloud computing (mean: 0.6074) and high-speed infrastructure (mean: 0.4207). This cluster is characterized by a *moderate level of digitalisation*. Cluster 3, consisting of 742 SMEs, demonstrates a lower level of digital technology integration, primarily relying on cloud computing (mean: 1.000) and high-speed technologies (mean: 0.3464). It can be concluded that Cluster 3 has a *low level of digitalisation*. Lastly, Cluster 2 (comprising 1360 SMEs) displays the lowest level of technology integration, with no particular technology standing out significantly. This cluster is associated with a *very low level of digitalisation*.

[2] Ibrahim (2013) revises some methods for assessing the relative importance of input variables in artificial neural networks. These methods are based on Garson's algorithm, which uses the absolute values of the final connection weights when calculating variable contributions. $RI_x = \sum_{x=1}^{n} \frac{|w_{xy}\ w_{yz}|}{\sum_{y=1}^{m} |w_{xy}\ w_{yz}|}$ where RI_x is the relative importance of neuron x. $\sum_{y=1}^{m} w_{xy}\ w_{yz}$ represents the sum of the product of the final weights connection from input neurons to hidden neurons with the connnections from hidden neurons to output neurons.

Table 4
Results of regression analysis (obstacles and digital technologies).

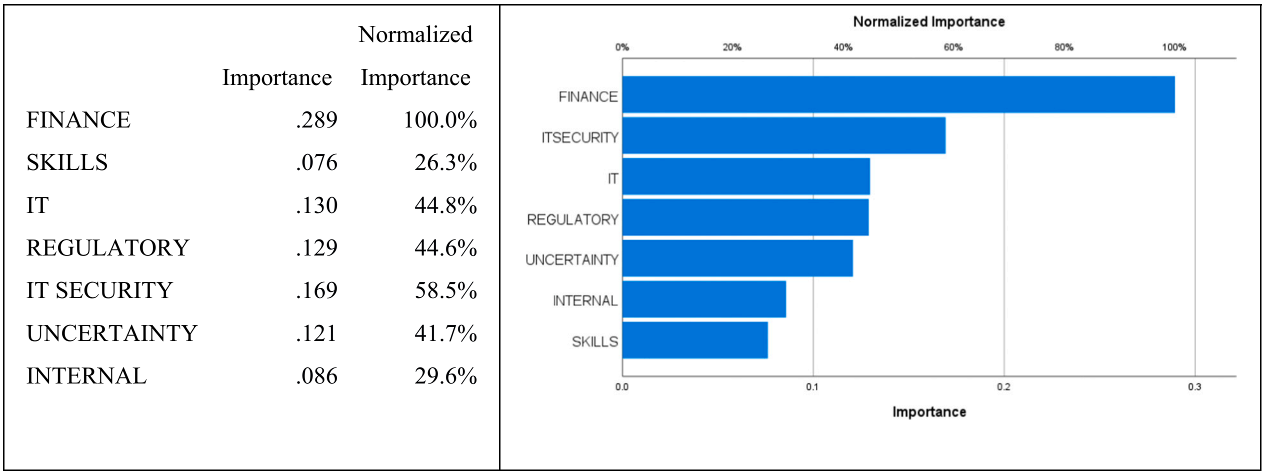
	AI	CLOUD	ROBOTICS	SMART	BIG DATA	HIGHSPEED	BLOCKCHAIN	VIF
FINANCE	−0.202	−0.126	−0.299**	−0.197*	−0.157	0.007	−0.248	1.07
SKILLS	0.038	0.135	0.024	0.097	−0.137	0.110	−0.316	1.16
IT	−0.433*	0.187	−0.152	0.245*	0.091	−0.620***	−0.470	1.08
REGULATORY	0.546**	0.094	0.090	0.275*	0.192	0.259*	0.328	1.14
IT SECURITY	0.784***	0.229*	0.521***	0.462***	0.507***	0.298**	0.548*	1.23
UNCERTAINTY	0.277	0.309**	0.066	0.079	−0.058	0.221*	0.298	1.25
INTERNAL	−0.129	0.463***	−0.463***	0.365***	0.561***	0.615***	0.211	1.14
−2 Log Likelihood	294.208	426.46	386.496	415.097	332.915	413.952	183.902	
Chi-Square	54.947	85.697	57.792	87.126	49.368	112.452	16.500	
Sig.	0.000	0.000	0.000	0.000	0.000	0.000	0.021	
Cox and Snell	0.017	0.027	0.018	0.027	0.015	0.035	0.005	
Nagelkerke	0.039	0.036	0.029	0.038	0.028	0.049	0.019	
McFadden	0.030	0.020	0.018	0.022	0.019	0.028	0.016	

* p < .05.
** p < .01.
*** p < .001.



	Importance	Normalized Importance
FINANCE	.112	55.9%
SKILLS	.080	40.3%
IT	.182	91.1%
REGULATORY	.119	59.6%
IT SECURITY	.200	100.0%
UNCERTAINTY	.109	54.6%
INTERNAL	.198	99.1%

Fig. 2. Results of ANN-MLP (obstacles and digitalisation).



	Importance	Normalized Importance
FINANCE	.289	100.0%
SKILLS	.076	26.3%
IT	.130	44.8%
REGULATORY	.129	44.6%
IT SECURITY	.169	58.5%
UNCERTAINTY	.121	41.7%
INTERNAL	.086	29.6%

Fig. 3. Results of ANN-MLP (obstacles and planning).

In Table 8, we see the results of the regression analysis. Thus, using Cluster 2 as a reference, which has a lower level of digital technologies, our results show that the rest of the clusters have a positive regression coefficient, showing a higher probability of digitalisation than Cluster 2. That is, regarding the level of digitalisation, we see that the cluster with a more positive coefficient value is Cluster 4 (β = 8.048, *p* < .001), followed by Clusters 1 (β = 3.678; *p* < .001) and 3 (β = 2.429; p < .001), showing a decrease in the level of digitalisation with respect to Cluster 2, confirming the results of the previous table that showed the variability in the level of digitalisation in SMEs. On the other hand, regarding future

Table 5
Results of K-mean analysis.

Number of Companies in each cluster		
Cluster	1	675
	2	1360
	3	742
	4	407
Valid		3184

Table 6
ANOVA results.

Digital technologies	F	Sig.
AI	101.777	0.000
CLOUD COMPUTING	2362.718	0.000
ROBOTICS	1770.505	0.000
SMART DEVICES	26,676.346	0.000
BIG DATA	124.681	0.000
HIGH SPEED	126.542	0.000
BLOCKCHAIN	27.966	0.000

planning, we see that the cluster with a more positive coefficient value is Cluster 4 (β = 1.826; p < .001), followed by Cluster 1 (β = 0.916; p < .001). 001) and 3 (β = 0.901; p < .001). In this same line, in Table 8, we show the probability of IT security issues in each cluster. Thus, it is confirmed that Cluster 4 (β = 1.088; p < .001) is the one with the highest probability of IT security issues, followed by Clusters 1 (β = 0.639; p < .001) and 3 (β=. 342; p < .001). These results confirm that IT security issues are more likely to be present in companies with a higher level of digitalisation. Additionally, in Fig. 5, we see the representation of the average values of IT security for each cluster.

Finally, along the same lines as the previous analysis, we have analysed the rest of the obstacles in reference to the cluster to which the SMEs belong (Table 9). Thus, we see that there is variability in the perception of obstacles depending on the cluster to which the SME belongs, and as a consequence of the level of digitalisation. Using Cluster 4, with a higher level of digitalisation, as a reference, the results show that Cluster 2, with a lower level of digitalisation, is the one with a higher probability of perceiving the obstacles than the rest of the clusters.

5. Discussion

This paper analyses the relationship between IT security and the digitalisation of SMEs in manufacturing. Our study explores this question, employing a sample of 3184 SMEs in the manufacturing sector.

Regarding the first research question (RQ1), about the effect that IT security issues have on the digitalisation of companies, our results show that IT security issues positively affect the digitalisation of companies. First, our results confirm previous works that show that SMEs are targets

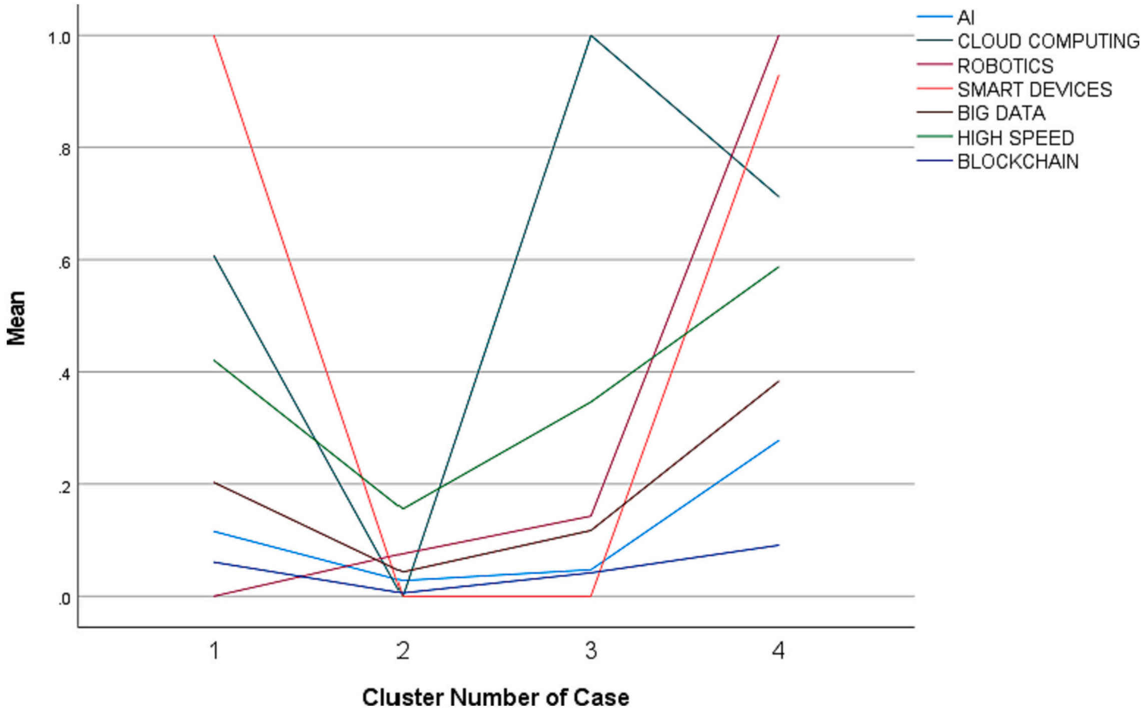


Fig. 4. Distribution of digital technologies in each cluster (Mean).

Table 7
Distribution of digital technologies in each cluster (Mean).

	CLUSTER1		CLUSTER2		CLUSTER3		CLUSTER4	
	Mean	Std. deviation	Mean	Std. deviation	Mean	Std. deviation	Mean	Std. deviation
AI	0.1156	0.31993	0.0279	0.16486	0.0472	0.21214	0.2776	0.44839
CLOUD COMPUTING	0.6074	0.48869	0.0000	0.00000	1.0000	0.00000	0.7125	0.45314
ROBOTICS	0.0000	0.00000	0.0757	0.26467	0.1429	0.35016	1.0000	0.00000
SMART DEVICES	1.0000	0.00000	0.0000	0.00000	0.0000	0.00000	0.9287	0.25756
BIG DATA	0.2030	0.40250	0.0434	0.20379	0.1173	0.32194	0.3833	0.48679
HIGH SPEED	0.4207	0.49404	0.1559	0.36288	0.3464	0.47613	0.5872	0.49294
BLOCKCHAIN	0.0607		0.0059	0.07650	0.0418	0.20022	0.0909	0.28783

Table 8
Results of regression analysis (Cluster).

	Digitalisation		Planning		IT security	
	Estimate	Std. Error			Estimate	Std. Error
CLUSTER 1	3.678***	0.140	0.916***	0.127	0.639***	0.146
CLUSTER 2	0[a]	–	0[a]	–	0[a]	–
CLUSTER 3	2.429***	0.131	0.901***	0.123	0.342*	0.144
CLUSTER 4	8.048***	0.198	1.826***	0.130	1.088***	0.138**
−2 Log Likelihood	268.290		86.835		26.154	
Chi-Square	3606.444		262.540		72.358	
Sig.	0.000		0.000		0.000	
Cox and Snell	0.678		0.100		0.022	
Nagelkerke	0.703		0.109		0.037	
McFadden	0.342		0.042		0.025	

[*] p < .05.
[**] p < .01.
[***] p < .001.

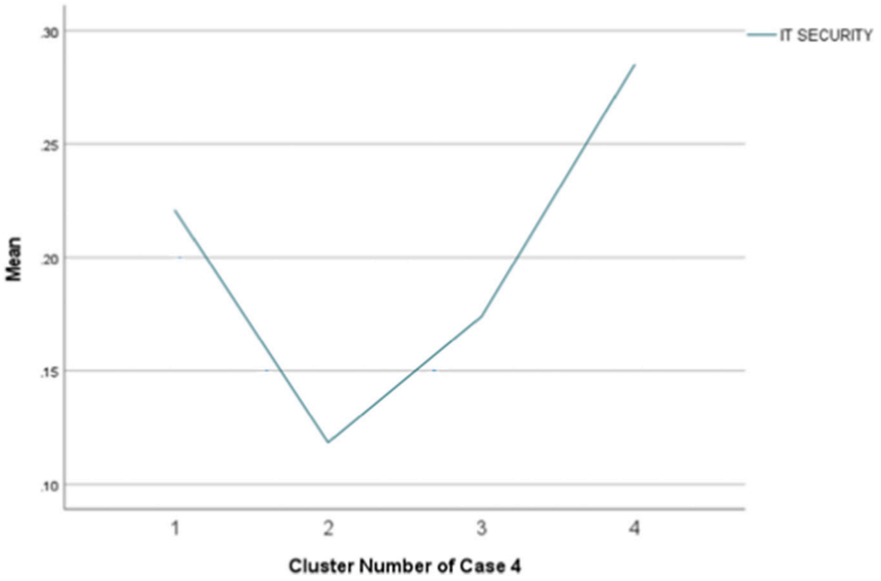


Fig. 5. Distribution of the effect of IT security issues/cluster.

Table 9
Regression analysis cluster/obstacles.

	Finance		Skills		IT		Regulatory		Uncertainty		Internal	
	Estimate	Std. error	Estimate	Std. error	Estimate	Std. error	Estimate	Std. error	Estimate	Std. error	Estimate	Std. error
CLUSTER 1	0.459**	0.153	−0.111	0.140	0.311	0.166	0.003	0.165	0.074	0.146	0.288*	0.141
CLUSTER 2	0.239	0.142	0.530***	0.129	0.365*	0.161	0.643***	0.159	0.686***	0.138	0.933***	0.133
CLUSTER 3	0.410**	0.152	0.173	0.138	0.063	0.168	0.271	0.168	−0.103	0.144	0.419**	0.140
CLUSTER 4	0[a]	.	0[a]	.	0[a]		0[a]	.	0[a]	.	0[a]	.
−2 Log Likelihood	26.822		26.954		25.598		25.300		26.504		26.594	
Chi-Square	11.820		25.334		29.456		29.091		44.861		60.591	
Sig.	0.008		0.000		0.000		0.000		0.000		0.000	
Cox and Snell	0.004		0.008		0.009		0.009		0.014		0.019	
Nagelkerke	0.006		0.012		0.016		0.017		0.022		0.030	
McFadden	0.003		0.007		0.011		0.012		0.014		0.019	

[*] p < .05.
[**] p < .01.
[***] p < .001.

of attacks, either directly, as a system to access interconnected companies in their supply chain, or of automatic attacks, as opposed to the perception of the managers of the SMEs who consider that their companies are exempt from cyber-attacks (Fernandez de Arroyabe and Fernandez de Arroyabe, 2021). Second, our work extends previous literature on the barriers to the digital transformation of SMEs (Masood and Sonntag, 2020; Orzes et al., 2018), pointing out that not all obstacles or barriers to digitalisation have a negative effect on digitalisation, but they can be perceived as challenges that motivate the promotion of digitalisation. Thus, in line with D'Este et al. (2012) in his study on the adoption of innovation in companies, it can be considered that the challenges that companies face in the innovation process can be perceived in a differential way for the companies. Thus, this author distinguished between two types of barriers to the adoption of innovation in companies: revealed barriers and deterrent barriers. While the first supposes a challenge that the company can overcome through learning and experience, the second refers to a barrier that companies see as an insurmountable one, and that sometimes does not allow continuation with the process. Therefore, regarding the role that IT security issues play in the digitalisation process, we can conceptualize them as revealed barriers, playing an important role in the digital transformation process. That is, the existence of IT security issues, for example, encourages companies to invest in cloud computing, to mitigate vulnerabilities against possible cyber-attacks. Lastly, our results show variability in the obstacles and the levels of digitalisation. Thus, compared with studies that indicated that SMEs suffered from financial, knowledge or management obstacles (see, for example, Orzes et al., 2018), we see that there is a differential impact on the perception of obstacles by SMEs depending on the level of digitalisation, both in the typology of the obstacles, as in their impact, and the dissuasive barriers to digitalisation challenges.

Regarding the second research question (RQ2), our results extend the literature, showing how I4.0 is being implemented in SMEs in manufacturing. Thus, our results show heterogeneity of levels of digitalisation, with a wide spectrum, from companies which, in terms of Masood and Sonntag (2020), integrate digital technologies with a variety of complexity, such as cooperative robots, cloud computing or smart devices, for example, to a group of companies that are incipient in the development of I4.0. Firstly, as differential aspects between the four groups of companies obtained, we see the first group of SMEs that, in terms of Clim (2019), represents a high level of implementation of I4.0, where the IIoT has been implanted, combined with sensors and robots. The main digital technology in this group is collaborative robots, including an interface for digital data collection and communication with external cloud platforms, with the objective of processing and acquiring data, contributing to creating collaborating robotic systems for smart production (Wang et al., 2022; Židek et al., 2020; Peixoto and Costa, 2017). The second group of companies has a lower level of digitalisation, where the use of smart devices prevails in their production process, combined with external data management, using cloud computing. A third group has more basic digitisation, and the main digital technology is reflected in the use of cloud computing. They are companies that in terms of Židek et al. (2020) control installations remotely, and combine data storage with data collection systems, using sensors and actuators connected with the controller via a wireless network. Lastly, a group of companies with little or no level of digitalisation have not yet joined the challenge of I4.0. In general, we can note that existing literature argues for the presence of these differences among companies, stemming from both external and internal factors within firms. For instance, Masood and Sonntag (2020) previously highlighted that the possession of competencies and skills within a firm is a crucial factor for its digitalisation. Ardito et al. (2021) emphasized that the required competencies are especially critical for SMEs, as these companies typically have a limited number of employees, and due to the integration and specificity of digital technologies, the adoption of such technologies can expose employees to a variety of specific tasks and learning experiences (Ardito et al., 2021). On the other hand, recent studies have pointed out the role of the supply chain as a driver of company digitalisation (Benitez et al., 2020; Kahle et al., 2020; Moeuf et al., 2018). The pressure exerted by clients and suppliers affects a company's digitalisation, both in terms of information exchange and production efficiency (Moeuf et al., 2018). Secondly, with common aspects that characterize the implementation of I4.0 in manufacturing SMEs, our results confirm previous work, in which companies transfer the burden of IT services from the local computer to the cloud, resulting in greater reliability (Ervural and Ervural, 2018; Kamel and Hegazi, 2018). Moreover, to store and analyse data, I4.0 devices are connected to the cloud and have as data sources sensors, actuators, PLCs, industrial robots, production equipment (for example, CNC milling machines) and mobile robots (Ani et al., 2016).

Moreover, our results show that the effect of IT security issues is heterogeneous, with a parallel effect between the degree of digitalisation and IT security. Fernandez de Arroyabe and Fernandez de Arroyabe (2021) have pointed out that attacks are becoming more sophisticated and diversified every day; therefore, from our results, we can point out that the more complex and diversified the digital technologies are, the more the vulnerabilities and IT security issues of SMEs potentially increase. Thus, Clim (2019) points out a diversity of scenarios in an industrial environment with a wide range of cyber-attacks. There is the installation of corrupted software, which can crash all forms of logistics and production operations, IIoT attacks, sabotaging industrial robot communication, or attacks in the social engineering environment, where attackers will take advantage of attributes such as trust, help, fear and curiosity of the employees. In this line, Humayun (2021) point out the risks of being interconnected to the IIoT. Thus, these authors highlight that each layer of the IIoT architecture can be attacked, the most typical attack being the Denial of Service (DoS), where the wireless link is vulnerable to such an attack, which can be done in the form of signal distortion (Clim, 2019). Other attacks can be, for example, tampering attacks, where the attacker physically modifies the devices or communication links; wormhole attacks, where a tunnel is established between two nodes and packets are forwarded between one other; hijacking attacks, creating a session for each user when they login to any web service such as the cloud. Within this diversification and sophistication of attacks, we can find attacks on the cloud service provider, for data theft (for example, back-door attacks, password guessing and social engineering, Humayun, 2021). Our results corroborate previous work, which indicates that as a consequence of the diversity of potential vulnerabilities, companies deepen their cybersecurity measures, increasing the number of countermeasures, such as greater encryption in communications, separation of management and production networks and so on. In Fig. 6, we see the characterization of the companies according to their levels of digitalisation and IT security issues.

6. Conclusions

This study offers a comprehensive exploration of the intricate interplay between IT security and the digitalisation journey of small and medium-sized enterprises (SMEs) operating within the manufacturing sector. Our empirical investigation, encompassing a survey of 3184 manufacturing SMEs utilizing data from the European Union, has uncovered a range of significant implications for the realms of theory, practice, and policy. Our empirical insights and theoretical and practical contributions provide valuable insights for scholars, practitioners, and policymakers alike, emphasizing the pivotal role of IT security in the ongoing digital transformation journey of these enterprises.

6.1. Theoretical contributions

Our *first theoretical contribution* is situated within innovation adoption theory (Rogers et al., 2014; Hameed et al., 2012; Van Oorschot et al., 2018; Blanchard et al., 2013; Damanpour and Schneider, 2006;

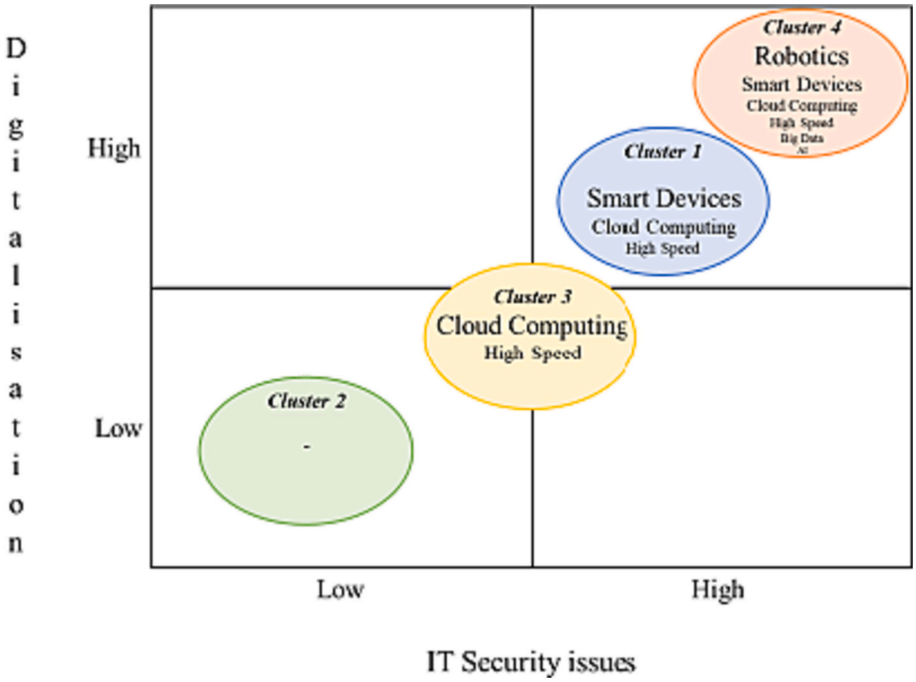


Fig. 6. Distribution of cluster by digitalisation level and IT security issues.

Frambach and Schillewaert, 2002). Traditionally, this theory posits that the implementation of innovations in companies constitutes a process fraught with inherent difficulties and barriers. These difficulties may stem from internal factors, such as a lack of funding, knowledge, or resistance within the organization, or they may emanate from external factors, including environmental uncertainties and regulatory voids. Our research extends this perspective by highlighting that the process of implementing I4.0 within SMEs is not exempt from challenges and barriers. In particular, we emphasize that the interconnection of systems in the digitalisation transformation of SME manufacturing exposes them to cybersecurity risks. These risks encompass incidents that can inflict damage upon stored data or disrupt the overall operations of these companies. Consequently, our study underscores the pivotal role played by IT security issues in the digital transformation process. Furthermore, our results reveal a nuanced landscape of obstacles and varying levels of digitalisation. In contrast to studies that primarily pinpoint financial, knowledge, or management-related obstacles, our findings reveal that the perception of obstacles among SMEs varies depending on their digitalisation levels. This variation encompasses both the types of obstacles encountered and the degree to which they deter digitalisation endeavours.

The *second theoretical contribution* extends into the domain of digital transformation. Existing literature has consistently asserted that the digital transformation of companies pivots upon the integration of digital technologies. This integration involves the amalgamation of intelligent technology, storage systems, and smart production systems, facilitated by wireless sensor networks, communication protocols, distributed control systems, and cloud computing. Additionally, the literature has advocated for an ecosystem perspective when scrutinizing supply chains in the I4.0 context. This perspective underscores the importance of complex interactions within ecosystems, which can provide financial resources and competencies to SMEs. However, prior research primarily concentrated on the demand side, analysing obstacles and barriers related to the adoption of digital technologies. Our study, we emphasize that in these ecosystems, companies are susceptible to cybersecurity incidents that can impact their digital transformation efforts. Moreover, our findings reveal a heterogeneity in the levels of digitalisation, with a corresponding variability in the influence exerted by IT security issues at different digitalisation stages. Our research confirms that the relationship between these variables is nuanced and perturbed by various factors at each stage of digitalisation. Indeed, some SMEs initiate their digitalisation journey in response to cybersecurity incidents, while others, at more advanced stages, have developed competencies and organizational procedures to mitigate vulnerabilities against such incidents. This underscores the integral role of digitalisation procedures and capabilities in shaping cybersecurity measures.

6.2. *Practical implications*

Our study highlights a crucial consideration for *managers,* showing the principal role of cybersecurity in SMEs' digitalisation activities. While previous studies often framed cybersecurity as an operational function confined to IT departments, our research underscores that it should be regarded as a strategic imperative involving top-level management. The recognition of cybersecurity's strategic significance is vital for safeguarding SMEs against evolving cyber threats in an increasingly digitalised landscape. Furthermore, our study elucidates the interplay between digital transformation and the escalation of IT security concerns. SMEs operating in the manufacturing sector should view IT security as an integral component of the digitalisation process. As such, investing in the implementation of robust cybersecurity systems becomes imperative. These investments not only safeguard SMEs' digital assets but also contribute to the resilience and sustainability of their digitalisation initiatives in the long run.

Our study has significant implications for *policymakers*, emphasizing the need to integrate digitalisation and cybersecurity strategies, rather than treating them as separate policies. Our results also highlight the unique context of SMEs, whereby, noting the importance of having specific policies for SMEs that aim at support a cyber secure digital transformation process. To fortify the digital resilience of small and medium-sized enterprises (SMEs) in the manufacturing sector, policymakers should prioritize comprehensive cybersecurity initiatives. For instance, policymakers could invest in dedicated cybersecurity education and awareness programs tailored for SMEs or they could provide financial incentives, such as subsidies or tax breaks, to encourage SMEs to adopt robust cybersecurity systems, relieving their financial burden.

Governments could also serve as platforms that will facilitate the collaboration between SMEs and cybersecurity experts.

6.3. Limitations and future research

Like all research work, our paper is not exempt from limitations. The main potential limitation of our study is the reliance on survey data from the "Flash Eurobarometer No. 486" database. While this dataset provides valuable insights into a large number of manufacturing SMEs across the European Union, it is subject to certain limitations. Firstly, the data is self-reported by SMEs, which may introduce response bias and subjective interpretations. Despite the robustness of the analysis with CMV, participants may provide responses that reflect their perceptions rather than objective assessments of IT security issues and digitalisation levels. Additionally, as the data is cross-sectional, it offers a picture of the SMEs' IT security and digitalisation status at a particular point in time.

For future research, we would recommend combining cross-sectional with longitudinal studies. Thus, longitudinal data tracking changes over time could provide deeper insights into the dynamics of these processes. Furthermore, our study primarily relies on quantitative data and machine learning methodology. While this approach offers valuable statistical insights, it may not fully capture the qualitative aspects and contextual nuances of IT security challenges and digitalisation efforts in SMEs. For future research, complementing the findings with qualitative research methods, such as interviews or case studies, could provide a more holistic understanding of these phenomena.

CRediT authorship contribution statement

Marta F. Arroyabe: Conceptualization, Formal analysis, Funding acquisition, Investigation, Methodology, Supervision, Writing – original draft, Writing – review & editing. **Carlos F.A. Arranz:** Conceptualization, Formal analysis, Investigation, Methodology, Software, Writing – original draft, Writing – review & editing. **Ignacio Fernandez de Arroyabe:** Conceptualization, Formal analysis, Investigation, Methodology, Supervision, Writing – original draft, Writing – review & editing. **Juan Carlos Fernandez de Arroyabe:** Conceptualization, Formal analysis, Investigation, Methodology, Software, Supervision, Writing – original draft.

Declaration of competing interest

The authors declare that they have no known conflict of interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

References

Alpaydin, E., 2021. Machine Learning. Mit Press.

Ani, U.P.D., He, H., Tiwari, A., 2016. Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. J. Cyber Secur. Technol. 1 (1), 32–74.

Ardito, L., Raby, S., Albino, V., Bertoldi, B., 2021. The duality of digital and environmental orientations in the context of SMEs: implications for innovation performance. J. Bus. Res. 123, 44–56.

Arranz, N., Fernandez de Arroyabe, J.C., 2010. Efficiency in technological networks, an approach from Artificial Neural Networks (ANN). Int. J. Manag. Sci. Eng. Manag. 5, 453–460.

Arranz, N., Arguello, N.L., Fernandez de Arroyabe, J.C., 2021. How do internal, market and institutional factors affect the development of eco-innovation in firms? J. Clean. Prod. 297, 126692.

Babbar, G., Bhushan, B., 2020. Framework and methodological solutions for cyber security in industry 4.0. In: Proceedings of the International Conference on Innovative Computing & Communications (ICICC). Available at SSRN. https://ssrn.com/abstract=3601513.

Bai, C., Quayson, M., Sarkis, J., 2021. COVID-19 pandemic digitization lessons for sustainable development of micro-and small-enterprises. Sustain. Prod. Consump. 27, 1989–2001.

Benitez, G.B., Ayala, N.F., Frank, A.G., 2020. Industry 4.0 innovation ecosystems: an evolutionary perspective on value cocreation. Int. J. Prod. Econ. 228, 107735.

Bishop, C.M., 1995. Neural Networks for Pattern Recognition. Oxford university press.

Blanchard, P., Huiban, J.P., Musolesi, A., Sevestre, P., 2013. Where there is a will, there is a way? Assessing the impact of obstacles to innovation. Ind. Corp. Chang. 22 (3), 679–710.

Brenner, B., Hartl, B., 2021. The perceived relationship between digitalization and ecological, economic, and social sustainability. J. Clean. Prod. 315, 128128.

Brunswicker, S., Vanhaverbeke, W., 2015. Open innovation in small and medium-sized enterprises (SMEs): external knowledge sourcing strategies and internal organizational facilitators. J. Small Bus. Manag. 53 (4), 1241–1263.

Ciurana, J., Quintana, G., Garcia-Romeu, M.L., 2008. Estimating the cost of vertical high-speed machining centers, a comparison between multiple regression analysis and the neural approach. Int. J. Prod. Econ. 115, 171–178.

Clim, A., 2019. Cyber security beyond the industry 4.0 era. A short review on a few technological promises. Inform. Econ. 23 (2), 34–44.

Da Silva, V.L., Kovaleski, J.L., Pagani, R.N., Silva, J.D.M., Corsi, A., 2020. Implementation of industry 4.0 concept in companies: empirical evidences. Int. J. Comput. Integ. Manuf. 33 (4), 325–342.

Damanpour, F., Schneider, M., 2006. Phases of the adoption of innovation in organizations: effects of environment, organization and top managers. Br. J. Manag. 17 (3), 215–236.

de Sousa Jabbour, A.B.L., Jabbour, C.J.C., Foropon, C., Godinho Filho, M., 2018. When titans meet–can industry 4.0 revolutionise the environmentally-sustainable manufacturing wave? The role of critical success factors. Technol. Forecast. Soc. Chang. 132, 18–25.

D'Este, P., Iammarino, S., Savona, M., von Tunzelmann, N., 2012. What hampers innovation? Revealed barriers versus deterring barriers. Res. Policy 41 (2), 482–488.

Díaz-Chao, Á., Ficapal-Cusí, P., Torrent-Sellens, J., 2021. Environmental assets, industry 4.0 technologies and firm performance in Spain: a dynamic capabilities path to reward sustainability. J. Clean. Prod. 281, 125264.

Dudek, A., 2020. Silhouette index as clustering evaluation tool. In: Classification and Data Analysis: Theory and Applications 28. Springer International Publishing, pp. 19–33.

Ervural, B.C., Ervural, B., 2018. Overview of cyber security in the industry 4.0 era. In: Industry 4.0: Managing The Digital Transformation, Cham, Switzerland. Springer, Cham, pp. 267–284.

Eurostat, 2022. Flash Eurobarometer 486: SMEs, start-ups, scale-ups and entrepreneurship. http://data.europa.eu/euodp/en/data/dataset/S2244_486_ENG.

Fernandez de Arroyabe, I., Fernandez de Arroyabe, J.C., 2021. The severity and effects of cyber-breaches in SMEs: a machine learning approach. Enterp. Inf. Syst. 1–27.

Fernandez de Arroyabe, J.C., Arroyabe, M.F., Fernandez, I., Arranz, C.F., 2023. Cybersecurity resilience in SMEs. A machine learning approach. J. Comput. Inf. Syst. 1–17.

Fraley, C., Raftery, A.E., 1998. How many clusters? Which clustering method? Answers via model-based cluster analysis. Comput. J. 41 (8), 578–588.

Frambach, R.T., Schillewaert, N., 2002. Organizational innovation adoption: a multi-level framework of determinants and opportunities for future research. J. Bus. Res. 55 (2), 163–176.

Frank, A.G., Dalenogare, L.S., Ayala, N.F., 2019. Industry 4.0 technologies: implementation patterns in manufacturing companies. Int. J. Prod. Econ. 210, 15–26.

Galati, F., Bigliardi, B., 2019. Industry 4.0: emerging themes and future research avenues using a text mining approach. Comput. Ind. 109, 100–113.

Goerzig, D., Bauernhansl, T., 2018. Enterprise architectures for the digital transformation in small and medium-sized enterprises. Proc. Cirp 67, 540–545.

Hameed, M.A., Counsell, S., Swift, S., 2012. A conceptual model for the process of IT innovation adoption in organizations. J. Eng. Technol. Manage. 29 (3), 358–390.

Harish, A.R., Liu, X.L., Zhong, R.Y., Huang, G.Q., 2021. Log-flock: a blockchain-enabled platform for digital asset valuation and risk assessment in E-commerce logistics financing. Comput. Ind. Eng. 151, 107001.

Hegazy, T., Fazio, P., Moselhi, O., 1994. Developing practical neural network applications using back-propagation. Comput.-Aided Civ. Infrastruct. Eng. 9 (2), 145–159.

Horváth, D., Szabó, R.Z., 2019. Driving forces and barriers of industry 4.0: do multinational and small and medium-sized companies have equal opportunities? Technol. Forecast. Focial Chang. 146, 119–132.

Humayun, M., 2021. Industry 4.0 and cyber security issues and challenges. Turk. J. Comput. Math. Educ. 12 (10), 2957–2971.

Ibrahim, O.M., 2013. A comparison of methods for assessing the relative importance of input variables in artificial neural networks. J. Appl. Sci. Res. 9 (11), 5692–5700.

Kahle, J.H., Marcon, É., Ghezzi, A., Frank, A.G., 2020. Smart products value creation in SMEs innovation ecosystems. Technol. Forecast. Soc. Chang. 156, 120024.

Kamel, S.O.M., Hegazi, N.H., 2018. A proposed model of IoT security management system based on a study of internet of things (IoT) security. Int. J. Sci. Eng. Res. 9 (9), 1227–1244.

Kass, R.E., Raftery, A.E., 1995. Bayes factors. J. Am. Stat. Assoc. 90 (430), 773–795.

Kotuszewski, P., Kukielka, K., Kluk, P., Ordys, A., Bieńkowski, K., Kościelny, J.M., Fajdek, B., 2021. Cyber-security assessment of industry 4.0 enabled mechatronic system. Complexity 6670625. https://doi.org/10.1155/2021/6670625.

Liao, Y., Deschamps, F., Loures, E.D., Ramos, L.F., 2017. Past, present and future of industry 4.0-a systematic literature review and research agenda proposal. Int. J. Prod. Res. 55 (12), 3609–3629.

Lu, Y., 2017. Industry 4.0: a survey on technologies, applications and open research issues. J. Ind. Inf. Integr. 6, 1–10.

Mamat, A.R., Mohamed, F.S., Mohamed, M.A., Rawi, N.M., Awang, M.I., 2018. Silhouette index for determining optimal k-means clustering on images in different color models. Int. J. Enginery Technol. 7 (2), 105–109.

Masood, T., Sonntag, P., 2020. Industry 4.0: adoption challenges and benefits for SMEs. Comput. Ind. 121, 103261.

Masters, T., 1993. Practical Neural Network Recipes in C++. Morgan Kaufmann.

Matt, D.T., Rauch, E., 2013. Implementation of lean production in small sized enterprises. Procedia Cirp 12, 420–425.

Mirtsch, M., Kinne, J., Blind, K., 2020. Exploring the adoption of the international information security management system standard ISO/IEC 27001: a web mining-based analysis. IEEE Trans. Eng. Manag. 68 (1), 87–100.

Mittal, S., Khan, M.A., Romero, D., Wuest, T., 2018a. A critical review of smart manufacturing & industry 4.0 maturity models: implications for small and medium-sized enterprises (SMEs). J. Manuf. Syst. 49, 194–214.

Mittal, S., Romero, D., Wuest, T., 2018b. Towards a smart manufacturing maturity model for SMEs (SM 3 E). In: IFIP International Conference on Advances in Production Management Systems. Springer, Cham, pp. 155–163.

Moeuf, A., Pellerin, R., Lamouri, S., Tamayo-Giraldo, S., Barbaray, R., 2018. The industrial management of SMEs in the era of industry 4.0. Int. J. Prod. Res. 56 (3), 1118–1136.

Mohrotra, K., 1994. Elements of Artificial Neural Networks. MA, MIT Press, Cambridge.

Morkunas, V.J., Paschen, J., Boon, E., 2019. How blockchain technologies impact your business model. Bus. Horiz. 62 (3), 295–306.

Müller, J.M., Buliga, O., Voigt, K.I., 2018. Fortune favors the prepared: how SMEs approach business model innovations in industry 4.0. Technol. Forecast. Soc. Chang. 132, 2–17.

Nounou, A., Jaber, H., Aydin, R., 2022. A cyber-physical system architecture based on lean principles for managing industry 4.0 setups. Int. J. Comput. Integr. Manuf. 1–19.

Orzes, G., Rauch, E., Bednar, S., Poklemba, R., 2018. Industry 4.0 implementation barriers in small and medium sized enterprises: a focus group study. In: 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM) (1348-1352). IEEE.

Pan, Ming, Sikorski, Janusz, Kastner, Catharine A., Akroyd, Jethro, Mosbach, Sebastian, Lau, Raymond, Kraft, Markus, 2015. Applying industry 4.0 to the Jurong Island eco-industrial park. Energy Procedia 75, 1536–1541.

Peixoto, J.P., Costa, D.G., 2017. Wireless visual sensor networks for smart city applications: a relevance-based approach for multiple sinks mobility. Futur. Gener. Comput. Syst. 76, 51–62.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.Y., Podsakoff, N.P., 2003. Common method biases in behavioral research: a critical review of the literature and recommended remedies. J. Appl. Psychol. 88 (5), 879.

Rauch, E., Dallasega, P., Matt, D.T., 2018. Complexity reduction in engineer-to-order industry through real-time capable production planning and control. Prod. Eng. 12 (3), 341–352.

Rogers, E.M., Singhal, A., Quinlan, M.M., 2014. Diffusion of innovations. In: An Integrated Approach to Communication Theory and Research. Routledge, pp. 432–448.

Russell, M.G., Smorodinskaya, N.V., 2018. Leveraging complexity for ecosystemic innovation. Technol. Forecast. Soc. Chang. 136, 114–131.

Sanchez, M., Exposito, E., Aguilar, J., 2020. Industry 4.0: survey from a system integration perspective. Int. J. Comput. Integr. Manuf. 33 (10–11), 1017–1041.

Sanders, A., Elangeswaran, C., Wulfsberg, J.P., 2016. Industry 4.0 implies lean manufacturing: research activities in industry 4.0 function as enablers for lean manufacturing. J. Ind. Eng. Manag. 9 (3), 811–833.

Schönfuß, B., McFarlane, D., Hawkridge, G., Salter, L., Athanassopoulou, N., De Silva, L., 2021. A catalogue of digital solution areas for prioritising the needs of manufacturing SMEs. Comput. Ind. 133, 103532.

Singh, A., Madaan, G., Hr, S., Kumar, A., 2022. Smart manufacturing systems: a futuristics roadmap towards application of industry 4.0 technologies. Int. J. Comput. Integr. Manuf. 1–18.

Stoldt, J., Trapp, T.U., Toussaint, S., Süße, M., Schlegel, A., Putz, M., 2018. Planning for digitalisation in SMEs using tools of the digital factory. Procedia Cirp 72, 179–184.

Thomas, A.J., Barton, R.A., 2012. Characterizing SME migration towards advanced manufacturing technologies. Proc. Inst. Mech. Eng. B J. Eng. Manuf. 226, 745–756.

Trappey, A.J., Trappey, C.V., Fan, C.Y., Hsu, A.P., Li, X.K., Lee, I.J., 2017. IoT patent roadmap for smart logistic service provision in the context of industry 4.0. J. Chin. Inst. Eng. 40 (7), 593–602.

Türkeş, M.C., Oncioiu, I., Aslam, H.D., Marin-Pantelescu, A., Topor, D.I., Căpuşneanu, S., 2019. Drivers and barriers in using industry 4.0: a perspective of SMEs in Romania. Processes 7 (3), 153.

Uygun, Ö., Aydin, M.E., 2021. Digital transformation: industry 4.0 for future minds and future society. Comput. Ind. Eng. 157, 107362.

Van Oorschot, J.A., Hofman, E., Halman, J.I., 2018. A bibliometric review of the innovation adoption literature. Technol. Forecast. Soc. Chang. 134, 1–21.

Vrchota, J., Mařiková, M., Řehoř, P., Rolínek, L., Toušek, R., 2019. Human resources readiness for industry 4.0. J. Open Innov. Technol. Market Complex. 6 (1), 3.

Wang, Q., 2007. Artificial neural networks as cost engineering methods in a collaborative manufacturing environment. Int. J. Prod. Econ. 109, 53–64.

Wang, Y., Wang, G., Anderl, R., 2016. Generic procedure model to introduce Industrie 4.0 in small and medium-sized enterprises. In: Proceedings of the World Congress on Engineering and Computer Science, Vol II WCECS 2016, San Francisco, USA.

Wang, J., Chen, J., Ren, Y., Sharma, P.K., Alfarraj, O., Tolba, A., 2022. Data security storage mechanism based on blockchain industrial internet of things. Comput. Ind. Eng. 164, 107903.

Woods, K., Bowyer, K.W., 1997. Generating ROC curves for artificial neural networks. IEEE Trans. Med. Imaging 16 (3), 329–337.

Yu, F., Schweisfurth, T., 2020. Industry 4.0 technology implementation in SMEs–A survey in the Danish-German border region. Int. J. Innov. Stud. 4 (3), 76–84.

Zhu, X., Ge, S., Wang, N., 2021. Digital transformation: a systematic literature review. Comput. Ind. Eng. 162, 107774.

Židek, K., Modrák, V., Pitel, J., Šoltysová, Z., 2020. The digitization of quality control operations with cloud platform computing technologies. In: Industry 4.0 for SMEs. Palgrave Macmillan, Cham, pp. 305–334.

Ignacio Fernandez de Arroyabe is Cyber Risk Manager in Lloyds Bank Commercial Banking (UK). He has worked in cybersecurity in Jaguar Land Rover in the UK. His research interests are in cybersecurity risk management in the firms. He is a PhD candidate in cybersecurity at Loughborough University.

Carlos F.A. Arranz is a Lecturer in Business Operations at the University of Greenwich. His main research interest centres on the application of Machine Learning methods to the analysis of business, particularly on the implementation of Circular Economy Models. He is author or co-author of numerous papers published in the *Technological Forecasting Social Change, R&D Management, Journal of Computer Information Systems, Computer & Security, Studies in Higher Education, Journal of Environmental Management, Journal Cleaner Production, Business Strategy and the Environment.* He is member of Business Analytics editorial board.

Marta F. Arroyabe is a Reader in Essex Business School (University of Essex). Her research interests include M&A, Innovation, Eco-innovation, and Cyber Security in SMEs. She is author or co-author of numerous papers published in the *British Journal of Management, R&D Management, Technological Forecasting Social Change, Scandinavian Journal of Tourism and Studies Higher Education, R&D Management, Applied Economy, Technovation, Journal of Computer Information Systems, Computer & Security, Studies in Higher Education, Journal of Environmental Management, Journal Cleaner Production, Business Strategy and the Environment, Oxford Bulletin of Economics and Statistics, Journal Business Research.* Also, he is Associate Editor of the Journal of Entrepreneurship in Emerging Economies.

Juan Carlos Fernandez de Arroyabe is a Professor in Essex Business School (University of Essex). His research interests include joint R&D projects, R&D networks, and complex technological systems. He is author or co-author of numerous papers published in the *British Journal of Management, IEEE Transaction Engineering Management, the Complexity, Technovation, Studies in Higher Education, Journal Cleaner Production, Business Strategy and The Environment, Journal Business Research; Emergence: Organization and Complexity, Technological Forecasting Social Change, Journal of Enterprise Information Management, International Small Business Journal, European Journal of Work and Organisational Psychology, Scandinavian Journal of Tourism, and Industry Higher Education*. Also, he is Associate Editor of the Journal of Entrepreneurship in Emerging Economies and member of Editorial Board of Technological Forecasting Social Change.